GLANCY PRONGAY & MURRAY LLP
Joshua L. Crowell (#295411)
Vahe Mesropyan (#307244)
1925 Century Park East, Suite 2100
Los Angeles, California 90067
(310) 201-9150
jcrowell@glancylaw.com
vmesropyan@glancylaw.com

POMERANTZ LLP
Jeremy A. Lieberman (*pro hac vice*)
Emma Gilmore (*pro hac vice*)
Michael Grunfeld (*pro hac vice*)
600 Third Avenue
New York, New York 10016
(212) 661-1100
jalieberman@pomlaw.com
egilmore@pomlaw.com

Counsel for Plaintiffs and Lead Counsel for the Class

- additional counsel on signature page -

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE YAHOO! INC. SECURITIES LITIGATION

THIS DOCUMENT RELATES TO: ALL ACTIONS

Case No. 17-CV-00373-LHK

PLAINTIFFS' OPPOSITION TO DEFENDANTS' YAHOO! INC. AND MARISSA MAYER'S MOTION TO DISMISS THE SECOND AMENDED CLASS ACTION COMPLAINT

Date: May 3, 2018
Time: 1:30 p.m.
Place: Courtroom 8, 4th Floor
Judge: Hon. Lucy H. Koh

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Lead plaintiffs Ben Maher ("Maher") and Sutton View Partners LP ("Sutton View") and named plaintiff Nafiz Talukder ("Talukder") ("Plaintiffs") respectfully submit this memorandum of law in opposition to defendants[1] Yahoo! Inc. ("Yahoo" or the "Company") and Marissa Mayer's ("Mayer") motion to dismiss (ECF No. 75) (the "Motion," cited as "Mot. at __")[2] the Second Amended Class Action Complaint (ECF No. 70) (the "SAC," cited as "¶__").

INTRODUCTION

In 2013 and 2014, Yahoo suffered two of the largest data breaches in history (the "Data Breaches"). In the "2013 Data Breach" alone, the confidential personal information of all 3 billion Yahoo users was stolen. The "2014 Data Breach," which compromised the information of over 500 million Yahoo users, was the work of Russian state operatives. Yahoo's crown jewel and key source of advertising revenue is its huge base of monthly active users. Defendants and Yahoo's investors understood that a large-scale data breach would substantially impair that core asset and cause the Company serious financial harm. Federal, state, and international law require the disclosure of significant data breaches. Yahoo and the Individual Defendants, however, failed to disclose the Data Breaches for several years, not until late 2016. Defendants also knew but failed to disclose that Yahoo's information security was substandard, under-resourced, outdated, and ineffective, which allowed the Data Breaches to occur.

Yahoo's eventual disclosure of the Data Breaches sparked widespread public outcry. Congress, law enforcement agencies, and industry experts were all immediately suspicious of when Yahoo's executives knew of the breaches. Details have since emerged showing that Defendants had contemporaneous knowledge of Yahoo's inadequate information security and both of the Data Breaches that resulted. This evidence includes, among other things, the findings of an Independent Committee that Yahoo's Board of Directors (the "Board") appointed to investigate the breaches, including who knew what and when, and statements by FBI agents and Yahoo employees with

[1] "Defendants" are Yahoo, former Chief Executive Officer ("CEO") Mayer, former General Counsel ("GC") Ronald Bell ("Bell"), and Chief Information Security Officer ("CISO") Alex Stamos ("Stamos"). Mayer, Bell, and Stamos are the "Individual Defendants."

[2] Bell and Stamos have each joined the Motion. ECF Nos. 79-80.

firsthand knowledge of Defendants' actions.

Witness accounts, as reported in numerous articles, have also explained why Defendants kept the public in the dark about the Data Breaches for over two years. It was well known within the Company throughout the Class Period that Yahoo had serious security vulnerabilities that made it susceptible to hackers. These vulnerabilities were the result of Yahoo's deficient information security practices, particularly its poor methods of encrypting and storing user data. But security weaknesses were far from the only problem that Yahoo faced. Its main advertising business struggled mightily during the Class Period, as Yahoo lost its former glory to its competitors in the technology industry. Starting in 2014, Yahoo's most influential shareholders began pressuring it to sell its operating business to a company that would be better able to unlock the full value of Yahoo's user base.

Faced with this crisis, Mayer prioritized maintaining the size of Yahoo's user base over protecting users' data. She saw the goals of user satisfaction and protecting users' personal information as being in direct conflict. For example, cybersecurity measures typically make products operate more slowly or inconvenience users. Mayer consistently rejected Stamos' requests to make security improvements that would have prevented or reduced the impact of the Data Breaches because she feared these measures would drive users away.

Despite Defendants' knowledge of Yahoo's cybersecurity deficiencies, they continually touted Yahoo's supposedly best-in-class and "industry standard" security protocols during the Class Period. Defendants also represented that Yahoo had disclosed and would disclose significant data breaches. These statements were false and misleading in light of Yahoo's substandard security practices and Defendants' failure to disclose the Data Breaches. While Defendants were boasting about Yahoo's data protections, for years the Company was subjecting users to ongoing harm by refusing to take the simple step of resetting their passwords, despite the fact that they knew that at least 3 billion users were acutely vulnerable to cybertheft as a result of the Data Breaches.

Indeed, the Court has already credited many of these precise factual allegations in its ruling on a motion to dismiss a related customer class action. *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *45 (N.D. Cal. Aug. 30, 2017) (hereinafter "*Yahoo Customer Data*"). The Court ruled as a matter of law that certain of the same types of

representations at issue here were false and misleading, and that Yahoo knowingly concealed its deficient information security practices and the 2014 Data Breach.

Beginning in May 2015, and culminating with Yahoo's disclosures of the Data Breaches in late 2016, details concerning Yahoo's deficient cybersecurity practices began to emerge. As the market digested this news, Yahoo's stock price tumbled by over 31% during the Class Period.

STATEMENT OF FACTS

A. Yahoo did not practice what it preached on information security.

By the start of the Class Period, Defendants knew all too well how great a risk Yahoo faced of having its data breached through its security vulnerabilities. When Mayer took over as CEO in 2012, Yahoo had been suffering attacks by Russian hackers for years. ¶¶91-93. Yahoo, along with other technology companies, was also attacked by Chinese military hackers in 2010. ¶63, 91. Unlike its peers, Yahoo never publicly admitted that breach and never committed the resources necessary to prevent future attacks. ¶64. In 2012, Yahoo suffered another breach, this time through a well-known type of attack that Yahoo could have prevented had it employed very basic and industry standard safeguards. ¶¶67-72. The perpetrators intended that breach to be a "wake up call" regarding Yahoo's well-known security holes. ¶73. Then, in 2013, Edward Snowden leaked information showing Yahoo was a frequent target of nation-state spies. ¶91.

Defendants, however, had competing interests that outweighed fixing these known security risks. Yahoo's core advertising business performed terribly during Mayer's time in charge, beginning in 2012. ¶¶48-49, 54-56, 90-91. As a result of Yahoo's deteriorating performance and financial missteps, in September 2014, Starboard Value LP, one of Yahoo's largest shareholders, urged the Company to drastically change course, such as by putting itself up for sale so that it could unlock the full value of its user base. ¶¶51, 52. Yahoo ended up agreeing in July 2016 to sell its core operating business to Verizon for approximately $4.48 billion—reflecting a whopping $350 million discount after Verizon learned of the Data Breaches. ¶¶57-58, 239. Several Yahoo information security employees recently explained that Yahoo's level of data security was so outdated at the time of the Data Breaches because Mayer saw the goals of data security and maintaining Yahoo's user base as being in direct conflict. ¶¶87-92. Increasing user protections would have made Yahoo's products

"slower and more difficult to use." ¶¶91. She personally rejected even the most basic security measures proposed by Stamos and his team because she feared that they would alienate Yahoo's user base that was so critical to its continued viability. ¶¶87-92. Mayer also wanted to avoid the cost of these improvements. *Id*.

For example, a very basic security failing was that Yahoo stored user data, such as passwords, with an encryption protocol called MD5 that was known since at least 2008 to be "cryptographically broken and unsuitable for further use." ¶¶86, 89, 97, 108, 410. Additionally, at the time of the 2013 Data Breach, Yahoo did not encrypt users' passwords and merely stored that information in plain text, which was befuddling to security experts. ¶72. Security experts blamed the 2012 data breach before the Class Period on Yahoo's use of this obsolete storage method, which they called an "altogether braindead idea." ¶87. The Court has credited allegations that these acts amounted to "fail[ures] to put in place reasonable security measures to protect user data." *Yahoo Customer Data*, 2017 WL 3727318, at *45. Industry experts have identified other cybersecurity failings at Yahoo, including the failure to secure servers containing user data, inadequate monitoring of network activity and intrusion-detection mechanisms, insufficient protections against email spam and phishing attacks, and keeping user data in a single database. ¶¶70-74, 87-94, 104, 410. Yahoo's substandard security practices even prompted the Company's peers to reach out directly to Mayer, informing her that Yahoo's lack of security is affecting their users and demanding Yahoo implement stronger encryption. ¶74. This second-rate information security culture that Mayer fostered caused key members of Yahoo's security team – including Stamos – to quit during the Class Period. ¶93.

B. Yahoo's deficient information security resulted in the Data Breaches.

Unsurprisingly, as a direct result of Yahoo's delinquent approach to information security, the Company suffered the Data Breaches at issue here. ¶92. During the 2013 Data Breach in August, hackers broke into Yahoo's email system and stole the Private Information of *3 billion users*. ¶97. This information was easily accessible to the hackers because it was secured by the outdated MD5 protocol discussed above. *Id.* Analysts called this breach "the Exxon Valdez of security breaches" and noted that it was the largest data breach from a single site in history. ¶¶107, 236. Then, according to an indictment brought by the Department of Justice ("DOJ"), in early 2014, two Russian intelligence

agents directed infamous hackers to steal Yahoo's users' Private Information. ¶110. In early 2014, the hackers breached Yahoo's network and began their reconnaissance. ¶111. In early 2014, they located, and later stole, Yahoo network resources, including Yahoo's user database ("UDB") and its account management tool ("AMT"), which Yahoo used to access information stored in the UDB. ¶¶108-11, 116-17. This data provided the hackers with the account information of at least 500 million Yahoo users, including data that was encrypted with the obsolete MD5 algorithm. ¶¶108-09, 116-17. The hackers also used phishing and spam marketing techniques to target the contacts of Yahoo's users and to access accounts of particular interest. ¶112. One of the hackers stole credit card information from users' email accounts and ran a sham advertising scam. *Id.* More recently, through 2016, these same hackers forged "cookies" that gave them widespread access to user email accounts (the "Forged Cookie Breach"). ¶¶197-201, 209. Cybersecurity experts and Yahoo's own employees agree that if Yahoo had better security measures, such as strengthened encryption of user data – in line with efforts that Defendants claimed to (but did not) employ – the Data Breaches would not have occurred or would have been far less severe. ¶¶87, 89-94, 104-07, 219-22, 227, 409.

The Independent Committee commissioned to investigate the 2014 Data Breach found in March 2017 that "the Company's information security team had ***contemporaneous knowledge*** of the 2014 compromise of user accounts, as well as incidents by the same attacker involving cookie forging in 2015 and 2016. In late 2014, ***senior executives and relevant legal staff were aware*** that a state-sponsored actor had accessed certain user accounts by exploiting the Company's account management tool . . . . Specifically, as of December 2014, the information security team understood that the attacker had exfiltrated copies of user database backup files containing the personal data of Yahoo users." ¶¶203-04 (emphasis added). The Committee largely blamed Bell, concluding that Yahoo's legal team "had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it." ¶213. Yahoo's main remedial actions in response to these findings were to penalize Mayer and Bell for their mishandling of the breach. Bell was forced to resign without pay and Mayer lost her cash bonus for 2016 and her 2017 annual equity award. ¶204. Stamos had already left Yahoo in 2015 because of his clashes with Mayer over security practices. ¶¶17, 93.

Further evidence shows that the Independent Committee's findings were actually understated

and that knowledge of the breaches was widespread throughout the Company. There is overwhelming evidence demonstrating that Stamos and his team detected the presence of Russian hackers in the Company's system as early as October 9, 2014. ¶130-31. For months, Stamos' team investigated the incident, which was internally named the "Siberian Intrusion," and even hired a third-party forensic expert to aid in the investigation. ¶130-31, 139. By December 2014, Yahoo's security team uncovered that Russian hackers had exfiltrated Yahoo user data. ¶¶142-43. Yahoo's Board, Mayer, and Bell routinely received updates about the investigation while it was ongoing. ¶¶134-36, 149-50. Stamos himself admitted that all material facts were reported and there was ample knowledge within the Company regarding the 2014 Data Breach. ¶148. Indeed, Stamos testified that Bell and Mayer had contemporaneous knowledge of the 2014 Data Breach. ¶151.

Others with firsthand knowledge have explained that Mayer was personally involved in efforts to resolve the Data Breaches and knew of their severity when they occurred. ¶¶205-08. The FBI agent in charge of investigating the 2014 Data Breach stated at a March 15, 2017 press conference that Mayer "and her team at Yahoo" were "great partners" during their two-year investigation. ¶205. Another FBI agent said they noticed right away clear signs that Russian hackers were behind the breach, including based on IP addresses near Moscow. ¶207.

Despite knowing of the Data Breaches, Defendants failed to employ even the most rudimentary corrective measures that would have minimized the threat to users' Private Information. A standard protective measure after a data breach is to instruct users to change their passwords. "Time is of the essence when" taking this type of protective step because "the more quickly we address the risks, the less harm an attack can cause." ¶¶44, 91-92, 121. As the Court has recognized, resetting user passwords here would have prevented much of the harm caused by the Data Breaches, yet Yahoo "delayed in notifying [customers] of the Data Breaches for a year to two years." *Yahoo Customer Data*, 2017 WL 3727318, at *41. The hackers used the "'nonce' associated with individual Yahoo user accounts" to mint cookies. ¶121. However, the DOJ's indictment explains that the hackers "could have been deterred from doing so if Yahoo had notified users and had them change their passwords" because the nonce associated with the users account changes when the user changes his or her password. *Id.* Even so, Mayer "rejected [this] most basic security measure" because, as with the other

measures discussed above, she "fear[ed] that even something as simple as a password change would drive Yahoo's shrinking email users to other services." ¶¶91, 417. Defendants constantly reassured the public of Yahoo's supposedly high level of protection of user data while knowing that hackers had ongoing access to account information because of Mayer's refusal to require password changes, leaving its customers acutely vulnerable to cybertheft.

Despite these failings, Mayer received a staggering $186 million in compensation during the Class Period, including over $51 million from Yahoo stock that she sold while in possession of nonpublic information regarding Yahoo's security deficiencies and the resulting Data Breaches. She also stood to receive a $23 million golden-parachute from the Verizon deal. ¶215.

C. Defendants finally disclose the Data Breaches.

Although Defendants knew of the Data Breaches by 2014, they did not disclose them publicly or instruct users to reset their email passwords to protect their Private Information until after Yahoo finalized its deal for Verizon to purchase its operating business. ¶¶57, 185. Defendants were even confronted in July and August 2016 by cybersecurity experts and reporters with evidence of vast amounts of user data being sold on the Internet, including to foreign state actors, but Defendants rebuffed these overtures and did not request additional information. ¶¶98-101, 167-73.[3]

Yahoo's belated bombshell disclosures of the Data Breaches prompted swift and dramatic reactions from all concerned constituencies. Congress, law enforcement agencies, Yahoo's users, industry experts, and Verizon, were all shocked by the historic scope of the breaches. They were also uniformly suspicious of the length of – and motivation for – Yahoo's delay in disclosing the breaches. ¶¶104, 194-95, 222-25, 227-28, 395, 398. Senators called on law enforcement agencies to "investigate whether Yahoo may have concealed its knowledge of [the 2014] breach in order to artificially bolster its valuation in its pending acquisition by Verizon." ¶¶194, 223. Yahoo is currently under civil or criminal investigation by the SEC, the DOJ, the Federal Trade Commission, several State Attorneys

[3] Defendants claim that an article discussing the July 2016 attempted sale of information from 200 million accounts references data stolen in 2012, not the Data Breaches. Mot. at 6 n.4. But Defendants ignore that Yahoo's investigation of this claim, which Mayer was involved in, led to Yahoo's admission two months later that it had contemporaneous knowledge of the 2014 Data Breach. ¶¶173 n.52, 186, 203.

General, and foreign governments investigating whether Yahoo took too long to disclose the breaches. ¶¶225-29. Several other Senators were concerned about Yahoo's "willingness to deal with Congress with complete candor" because Yahoo was "unable to provide answers to many basic questions." ¶228. In addition, at least 43 consumer class actions, and several shareholder derivative actions, have been filed against Yahoo related to the Data Breaches. ¶241. Verizon seriously considered canceling its purchase of Yahoo's operating business because the breaches constituted material adverse events under the sale agreement. ¶¶217, 230-34. Ultimately, Yahoo agreed to reduce the purchase price by $350 million and to be responsible for half of certain liabilities related to the breaches and other cybersecurity issues. ¶¶235-39.

Yahoo's disclosure of the Data Breaches had an immediate and significant negative impact on Yahoo's stock price. ¶¶394-99, 408-09. The market also reacted negatively after learning of many other disclosures, beginning in May 2015, that partially revealed Yahoo's inadequate data security efforts. ¶¶372-409. These earlier disclosures alerted the market to the fact that something was amiss with Yahoo's cybersecurity practices. The market then learned the full extent of those deficiencies when Yahoo finally disclosed the Data Breaches in late 2016.

ARGUMENT

When ruling on a "Rule 12(b)(6) motion to dismiss a §10(b) action, courts must . . . accept all factual allegations in the complaint as true." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007). While Plaintiffs must meet a heightened pleading standard under both Rule 9(b) and the PSLRA, "it is only under extraordinary circumstances that dismissal is proper under Rule 12(b)(6)." *In re China Educ. Alliance Sec. Litig.*, 2011 U.S. Dist. LEXIS 117416, at *8 (C.D. Cal. Oct. 11, 2011). A motion to dismiss must be denied where the complaint plausibly articulates the circumstances constituting fraud. *See Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

I. The SAC adequately alleges that Defendants made materially false and misleading statements and omissions during the Class Period.

The Ninth Circuit has long held that whether a "statement is misleading, or whether adverse facts were adequately disclosed[,] is a mixed question [for] the trier of fact." *Fecht v. Price Co.*, 70 F.3d 1078, 1081-82 (9th Cir. 1995). A case can be dismissed on this ground only if "'reasonable

minds' could not disagree that the challenged statements were not misleading." *Id.* Once defendants choose to speak positively about a topic, they are "bound to do so in a manner that wouldn't mislead investors as to potentially negative information within their possession." *Schueneman v. Arena Pharms., Inc.*, 840 F.3d 698, 707-08 (9th Cir. 2016) (internal quotation marks omitted).

A. Defendants' statements regarding information security contained misrepresentations and omissions.

1. Yahoo's statements regarding safeguards, best practices, and level of security were misleading because they failed to disclose its deficient information security and the Data Breaches.

Yahoo's Privacy Policy, posted on its website, represented that the Company had "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you," and "deploy[ed] industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect your personal information." ¶¶244, 302, 345, 347, 364, 366. In addition, Defendants represented that Yahoo was implementing "security best-practices," "provid[ing] the best possible protections," and "deploy[ing] the best possible technology to combat attacks and surveillance that violate our users' privacy." ¶255 (Sr. Vice Pres. Commc'n Prods., Oct. 14, 2013); ¶¶274-75 (Stamos, Apr. 2, 2014); ¶290 (Bell, June 5, 2014); ¶320 (official website, Mar. 26, 2015). Mayer boasted about "ensur[ing] that our products are as secure as possible" (¶279 (Apr. 15, 2014 earnings call)), and retweeted a press release stating that "Yahoo continues to provide the highest level of security possible to their users" (¶¶339-40 (Oct. 26, 2015)).

These statements were false and misleading because, in reality, Yahoo's measures "protecting" Private Information were obsolete and subjected Yahoo's users to the Data Breaches. And once the Data Breaches occurred, Yahoo refused to take the simple step of requiring its users to change their passwords, thereby leaving them especially exposed to cyber theft. Indeed, as a result of Yahoo's failure to notify users and direct them to change their passwords, the SAC alleges that the 2014 intrusion continued unabated until at least September 2016. ¶¶117, 121. Such statements describing Yahoo's cybersecurity practices in glowing terms were materially false and misleading. Yahoo actually employed severely deficient and outdated security practices because of Mayer's fear "that the inconvenience of added protection would make people stop using the company's products." ¶91.

Mayer even went so far as to deliberately refuse to take the basic step of requiring users to reset their passwords after the Data Breaches even though it would have prevented hackers from accessing nearly a billion users' accounts. ¶¶91-92. Thus, Defendants' public reassurances of the safety of user information, made while they knew that hackers were in the process of stealing user data – a direct result of Mayer's ongoing refusal to reset passwords – were false and misleading. Because of these false assurances, Defendants had a duty to disclose the Data Breaches. *See Schueneman*, 840 F.3d at 707 (holding that false assurances gave rise to duty to disclose).

In its analysis of the consumer plaintiffs' claims, the Court expressly determined that Yahoo's statement that it had "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you" was a misrepresentation. *Yahoo Customer Data*, 2017 WL 3727318, at *26. Rejecting Yahoo's argument that the statement was puffery, the Court stated that "a reasonable consumer could rely on this statement as representing that Defendants' safeguards, which were represented to comply with federal regulations, were sufficient to protect users' information from ordinary data security threats." *Id.* In so doing, the Court credited allegations that Yahoo's "privacy safeguards were not sufficient to protect users' information from ordinary data security threats"; for example, the Company's "'data encryption protocol' was 'widely discredited and had been proven, many years prior, easy to break.'" *Id.* at *26. The Court also ruled that other positive statements similar to those alleged in the SAC gave rise to a duty to disclose that Yahoo's "online security was non-compliant and substandard." *Id.* at *30.

Defendants' argument that the occurrence of the Data Breaches is not necessarily inconsistent with the above challenged statements has no merit. Mot. at 13. It ignores the allegations in the SAC that Yahoo was insufficiently committed to best practices, which led to deficient and substandard information security and ultimately resulted in the massive Data Breaches. The cases cited by Defendants (Mot. at 13-14) are inapplicable. In *Retail Wholesale & Dep't Store Union Local 338 Ret. Fund v. Hewlett-Packard Co.*, 845 F.3d 1268, 1276 (9th Cir. 2017), the corporate code of conduct at issue was not actionable because no company could reasonably represent that it would ensure the compliance of numerous individuals' personal behavior. In contrast, Yahoo did reasonably represent – falsely – that its information security would not be inadequate and substandard. And in *In re*

Heartland Payment Sys. Sec. Litig., 2009 U.S. Dist. LEXIS 114866, *4, 13-14, 18 (D.N.J. Dec. 7, 2009), the statements at issue were far more general, the company actually put substantial resources into improving security, and defendants disclosed the breach immediately after learning of its severity.

In addition, Defendants falsely assert that the only specific security deficiency alleged in the SAC relates to MD5 encryption. Mot. at 14. In reality, the SAC alleges other types of deficiencies: maintaining all user data in one database, the failure to secure servers containing user data, inadequate monitoring of network activity, the failure to implement intrusion-detection mechanisms for production systems, and insufficient protections against email spam and phishing attacks. ¶¶70-74, 86-94, 104, 410. The SAC cites several press reports – based on numerous interviews with Yahoo employees and industry experts – describing how Yahoo's data security fell behind that of its peers. ¶¶86, 89-91, 94, 104, 410. These reports specifically mention Mayer's decision to back-burner efforts to bolster data security. ¶¶89, 91, 104.

Finally, Defendants contend that many of the challenged statements above are inactionable puffery because they are vague, aspirational, or corporate optimism. Mot. at 19-20. But determining whether statements are puffery "'entails fact-intensive assessments that are more properly left to the jury.'" *Mulligan v. Impax Labs.*, 36 F. Supp. 3d 942, 966 (N.D. Cal. 2014). Defendants' representations that they employed "industry standard" or "best practices" are not puffery because they can be objectively measured against those standards. *In re EZCorp, Inc. Sec. Litig.*, 181 F. Supp. 3d 197, 206-08 (S.D.N.Y. 2016) (descriptions of compliance "with regulatory and industry best practices" were not puffery). *In re Sony Gaming Nets. & Cust. Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 990 (S.D. Cal. Jan. 21, 2014), is particularly instructive. The *Sony* court held, as to fraud claims arising out of data breaches, that whether representations of "'reasonable security' were deceptive, in light of additional representations regarding 'industry-standard' encryption, are questions of fact not suitable for" a motion to dismiss. *Id.*

Statements relating to a key aspect of the company's business are actionable when they represent a level of security vastly different from what actually existed. *See In re Volkswagen "Clean Diesel" Mktg., Sales Pracs., & Prods. Liab. Litig.*, 2017 U.S. Dist. LEXIS 112977, *687 (N.D. Cal. July 19, 2017) (holding statements that "'top priority' and 'focal point' for R&D was to" reduce

emissions were not puffery); *Bricklayers and Masons Local Union No. 5 Ohio Pension Fund v. Transocean Ltd.*, 866 F. Supp. 2d 223, 243-44 (S.D.N.Y. 2012) (statement that defendant "conducted 'extensive' training and safety programs" was actionable because "[i]n an industry as dangerous as deepwater drilling," investors are "greatly concerned" about "safety and training efforts"). When defendants constantly repeat these positive statements to allay specific concerns of the investing public, these representations are even more material. *See In re Petrobras Sec. Litig.*, 116 F. Supp. 3d 368, 381 (S.D.N.Y. July 30, 2015). Similarly, here, where data breaches posed one of Yahoo's most significant financial and operational risks, Defendants' repeated emphasis on, and investor assurance of, Yahoo's cybersecurity gave the false impression that users' information was secure even though hackers had unfettered access to their data.

2. Yahoo's representations in the Stock Purchase Agreement attached to its proxy statement were false.

In Yahoo's Stock Purchase Agreement with Verizon ("SPA"), signed by Mayer and attached to a proxy statement filed with the SEC on September 9, 2016, Defendants falsely represented that Yahoo had not suffered any data breaches or theft of personal data "that could reasonably be expected to have a Business Material Adverse Effect ['MAE']." ¶¶216, 359, 368-69. Yahoo further represented that it had not been required by law to notify anyone of any security breaches and that it did not know of any material government investigations related to personal data. *Id.* These statements were false because Yahoo had already suffered the Data Breaches and was required to disclose them. ¶¶96-201.

Defendants incorrectly argue that Yahoo's proxy statement disclaimed investor reliance on representations made in the SPA, stating that they "are not intended to be treated as categorical statements of fact." Mot. at 17. Merely inserting such boilerplate language does not immunize issuers from Rule 10b-5 liability, *see Quality Sys.*, 2017 U.S. App. LEXIS 13708, at *22-23, *36-40, and Defendants cite no authority holding otherwise. Just as in *Glazer Capital Mgmt., LP v. Magistri*, 549 F.3d 736, 741 (9th Cir. 2008), "[Yahoo] could have expected intense investor interest in the details of the merger," notwithstanding whatever generic disclaimers were in the agreement. *See also In re Bank of Am. Corp. Sec., Deriv., & ERISA Litig.*, 757 F. Supp. 2d 260, 299 (S.D.N.Y. 2010).

Defendants also unsuccessfully contend that Plaintiffs have not alleged that the representations

were false because there are no facts showing that the Data Breaches "met the MAE threshold." Mot. at 18. Yet Verizon's General Counsel and analysts stated that there was a reasonable basis to believe that the 2014 Data Breach had a material adverse impact on the deal. ¶¶217, 230-34. Yahoo was forced to lower the purchase price by $350 million and bear a substantial portion of liability from the breaches. ¶¶6, 239. This is strong evidence of a material "financial or business effect." Mot. at 18.

The argument that Plaintiffs did not rely on the SPA because they did not purchase Yahoo securities after the SPA had been publicly filed (Mot. at 18) is in Section III.C below.

3. Statements about information security risks were misleadingly incomplete and provided false assurances.

Yahoo and Mayer disclosed in all of Yahoo's periodic filings after the 2013 Data Breach that unspecified "[s]ecurity breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure."[4] This statement was materially misleading because it grossly downplayed the significance of the Data Breaches – the two largest in history, which Yahoo failed to disclose despite knowing that they had occurred. Particularly because Yahoo had previously disclosed smaller breaches within days after they occurred (¶¶67-68), a reasonable investor would understand that any significant past breaches had already been publicly disclosed.

Vague statements about unnamed past data breaches were therefore misleading because they failed to disclose the Data Breaches. *See In re Citigroup Inc. Sec. Litig.*, 753 F. Supp. 2d 206, 240 (S.D.N.Y. Nov. 9, 2010) (disclosure of $43 billion CDO liability was misleading because it failed to disclose additional $10.5 billion in indirect exposure); *In re Scottish Re Grp. Sec. Litig.*, 524 F. Supp. 2d 370, 389-90 (S.D.N.Y. 2007). The fact that Yahoo's stock reacted so negatively when the Data Breaches were later disclosed (¶¶394-99, 408-409) shows that Defendants' statements did not fully apprise the market of the existence and impact of past data breaches. *In re Juno Theraps.*, 2017 U.S. Dist. LEXIS 91608, at *17-18 (W.D. Wash. June 14, 2017); *Scottish Re*, 524 F. Supp. 2d at 389-90. Although Yahoo's reference to past breaches appeared in the risk factors section of its disclosures (Mot. at 15), the statement that "security breaches or unauthorized access have resulted in" financial consequences is an actionable statement of historical fact that cannot be cured by cautionary language.

[4] ¶¶268-69, 281-82, 294-93, 308-09, 313-14, 326-27, 331-32, 342-43, 349-50, 356-57, 361-62.

In re Atossa Genetics Inc. Sec. Litig., 2017 U.S. App. LEXIS 15658, at *26 (9th Cir. Aug. 18, 2017); *In re Quality Sys.*, 2017 U.S. App. LEXIS 13708, at *22-23, 36-40 (9th Cir. July 28, 2017).

The cases that Defendants cite concerning risk warnings are irrelevant because they did not address statements of historical fact. Mot. at 15. The warning language here was also far too general because it did not mention Yahoo's inadequate security efforts. *Atossa*, 2017 U.S. App. LEXIS 15658.

4. Statements about information security practices were misleadingly incomplete and provided false assurances.

Defendants repeatedly touted Yahoo's implementation of specific cybersecurity measures.[5] In light of the publicly disclosed breaches prior to the start of the Class Period, such statements constituted reassurances to Yahoo's customers and investors. These reassurances were false, however, because they failed to disclose Yahoo's deficient, substandard information security and the occurrence of the Data Breaches. Defendants argue that these statements are not actionable because they were unrelated to and not necessarily inconsistent with the Data Breaches. Mot. at 14-15.

Contrary to Defendants' assertion, the specific security measures that Yahoo touted are directly related to the infirmities in Yahoo's security practices that led to the Data Breaches. For example, when Mayer was asked at the World Economic Forum in March 2015 about public concern over the security of email data in light of Snowden's revelation that Yahoo was a frequent target for nation-state spies – as Yahoo was in the 2014 Data Breach – she stated that Yahoo built public trust by creating "entirely secure connections on all of . . . Yahoo's major properties," including better encryption methods. ¶316; *see also* ¶¶347, 366 (touting "secure storage" of users' information). In reality, however, Yahoo's method for encrypting and storing user data was "cryptographically broken and unsuitable for further use." ¶¶86, 89, 97, 108, 410.

Defendants' statements touting Yahoo's supposedly industry-leading efforts to combat malicious advertising, spam email, and phishing scams were also related to the Data Breaches. For example, Stamos testified before Congress in May 2014 that Yahoo was an industry leader in preventing a particularly malicious type of spam that is used for phishing attacks. ¶284; *see also* ¶287.

[5] *See* ¶¶244, 252, 254-55, 260, 264, 266, 271-72, 274-75, 277, 279, 284-88, 290, 292, 297-98, 300, 302-04, 306, 311, 316, 318, 320, 322, 324, 329, 334, 336, 338-40, 345-47, 352, 354, 364-67.

Despite these assurances, during the Data Breaches, hackers used malicious advertising, email spam, and phishing techniques to lure Yahoo's users into their schemes and to target their email contacts. ¶¶112, 241. The Court has credited allegations that the 2014 Data Breach began with phishing emails sent to Yahoo employees, and that a Yahoo customer received phishing emails as a result of the Data Breaches. *See Yahoo Customer Data*, 2017 WL 372318, at *14-15, *18-19; ¶108. Defendants' statements touting Yahoo's cybersecurity measures were therefore directly tied to the Data Breaches.

Further, Defendants' statements flooding the market with claims of Yahoo's robust cybersecurity measures – regardless of their specific subject – collectively misled investors by giving the overall impression that Yahoo employed very high cybersecurity standards. Defendants therefore had a duty to disclose the full picture of Yahoo's insufficient practices and the Data Breaches that followed. *See Meyer v. Jinkosolar Holdings Co., Ltd.*, 761 F.3d 245, 251 (2nd Cir. 2014) (holding description of pollution-prevention efforts "gave comfort to investors" and therefore, even if true, gave rise to a duty to disclose that these steps were "failing to prevent substantial [regulatory] violations"); *Stone v. Life Partners Holdings*, 26 F. Supp. 3d 575, 596, 599 (W.D. Tex. May 15, 2014). Defendants rely on inapposite cases where disclosures were expressly limited to specific topics and did not create a more comprehensive positive impression. Mot. at 15 (citing, *e.g.*, *Heartland*, 2009 U.S. Dist. LEXIS 114866, at *8-12, *16-23 (isolated statements were unrelated to data breach and did not create a misleading overall impression)).

5. Yahoo's press release on September 22, 2016 contained materially misleading omissions.

In contending that Yahoo's press release dated September 22, 2016 was not materially misleading, Defendants engage in serious hair-splitting. Mot. at 19. First, the press release stated that data exfiltration was discovered only through a "recent" investigation when in fact Yahoo had contemporaneous knowledge of the breaches. ¶186. Defendants weakly argue that this statement did not "signify that Yahoo was unaware of the intrusion prior to the [investigation]" (Mot. at 19), but that is clearly implied absent any acknowledgement of Yahoo's contemporaneous knowledge. Second, the press release stated that the stolen account information "*may have* included names, email addresses, telephone numbers, dates of birth, hashed passwords," when in fact they *had* been stolen. ¶188.

Defendants argue that this was technically true because there is no allegation that such information had been stolen from *every* account. Mot. at 19. But if Defendants had wanted to convey that without misleading anyone, they would have said that such information had been stolen from a portion of the accounts. Third, the press release stated that information was stolen by what Yahoo "believes is a state-sponsored actor," when in fact the Company *knew* it was Russia. ¶189. At this stage of the case, Defendants cannot show that no reasonable investor would consider this omission material. *See Mulligan*, 36 F. Supp. 3d at 966 ("[D]etermining whether a given statement is material 'entail[s] fact-intensive assessments that are more properly left to the jury.'").

B. Yahoo's representations gave rise to a duty to disclose the Data Breaches.

At least two categories of statements gave rise to Defendants' duty to disclose the Data Breaches: (1) Yahoo's vulnerability disclosure policy; and (2) Yahoo's representations of legal compliance. *See Schueneman*, 840 F.3d at 707-08 (holding that once defendants choose to speak positively about a topic, they are "bound to do so in a manner that wouldn't mislead investors as to potentially negative information within their possession").

Yahoo's website represented that it would publicly disclose all security vulnerabilities within 90 days of discovery and notify users "if we strongly suspect that your account may have been targeted by a state-sponsored actor." ¶¶2, 4, 39, 44-45. The Company's Privacy Policy, posted on its website throughout the Class Period, represented that Yahoo complied with federal regulations and industry standards for protecting user data. ¶¶244, 302, 345, 364. For this reason, investors expected Yahoo to comply with federal, state, and international laws requiring the disclosure of significant data breaches. Specifically, SEC guidance explains that the federal securities laws require the "disclosure of timely, comprehensive, and accurate information about [material cybersecurity] risks." ¶40. If a data breach is significant enough, a registrant cannot merely disclose a general risk but must rather describe the "specific attack and its known and potential costs and other consequences." *Id.* In determining whether a breach meets this standard, registrants must consider "the quantitative and qualitative magnitude" of the breach, including the possible consequences of misappropriation of sensitive data. ¶36. The Data Breaches here – the two largest in history – easily meet this threshold. Indeed, at the time of the 2014 Data Breach, the information security team members at Yahoo all

agreed that the intrusion represented a significant security breach. ¶137. And Dell SecureWorks, the third-party forensic expert Yahoo hired to aid with its investigation specifically concluded in its February 2, 2015 report presented to Yahoo that the 2014 intrusion was "large-scale" and exfiltrated user data from Yahoo's systems, including "user credentials for internal networks as well as VPN tokens for entering the network from the outside." ¶¶139-45.[6]

Affirmations of legal compliance are actionable when defendants violate the rules they adopted. *Glazer*, 549 F.3d at 742 (statements of compliance with securities laws was actionable); *In re Am. Apparel S'holder Litig.*, 2013 U.S. Dist. LEXIS 189797, at *45 (C.D. Cal. Aug. 8, 2013) (representations of "diligent efforts" to comply with immigration laws were false). *See also In re Omnicare, Inc. Sec. Litig.*, 769 F.3d 455, 479 (6th Cir. 2014) (finding a statement of "material compliance with federal, state, and local laws" to be actionable based on evidence that the defendant was not in compliance with those rules); *Omnicare, Inc. v. Laborers Dist. Council Constr. Indus. Pension Fund*, 135 S. Ct. 1318, 1333 (2015) (holding "legal compliance opinions" can give rise to a duty to disclose). Defendants' argument that SEC guidance and state law do not give rise to an independent duty to disclose (Mot. at 10-11) misses the point because it ignores that Defendants affirmatively adopted those rules by vouching that they complied with them. Thus, Defendants' concern about a supposedly "unprecedented" expansion of Rule 10b5-1 liability (Mot. at 11) is unfounded because liability here is premised on Yahoo's misleading representations of legal compliance and its vulnerability disclosure policy.

Defendants' argument that these policies and representations were directed not to investors but to individual users and "peers in the Internet community" (Mot. at 11-12) misses the mark for reasons stated in Section I.C.1 below. Regardless, even if the laws and Yahoo's policies required disclosure to users rather than to the public-at-large, notifying 3 billion users whose data was stolen is tantamount to disclosing the breaches publicly. By failing to notify its users, Yahoo effectively succeeded in concealing the Data Breaches from investors as well. To the extent that Yahoo's policy of not "shar[ing] any details publicly" about cyberattacks would not allow public notification, as Defendants

[6] Additionally, as Yahoo and Mayer told investors, "[m]any states have passed laws requiring notification to users where there is a security breach for personal data." ¶36

suggest (Mot. at 12), that would conflict with Yahoo's public disclosures of attacks shortly before the Class Period. ¶¶67-68.

C. Defendants' remaining arguments against falsity are without merit.

1. The challenged statements were made in connection with the purchase of or sale of Yahoo securities.

Defendants contend that many of the statements at issue, such as Yahoo's "customer-facing" policies, statements to security professionals, and blog posts, are not actionable because they were not made in connection with the purchase or sale of Yahoo securities. Mot. at 11, 20-21. This argument ignores the fundamental presumption that "the market price of shares traded on well-developed markets reflects *all publicly available information*, and, hence, any material misrepresentations." *Basic Inc. v. Levinson*, 485 U.S. 224, 246 (1988) (emphasis added). Courts regularly hold that publicly disclosed statements are made "regarding" securities transactions because "market professionals generally consider most publicly announced material statements." *In re Carter-Wallace, Inc. Sec. Litig.*, 150 F.3d 153, 156 (2d Cir. 1998); *Last Atlantis Cap. v. AGS Spec. Parts.*, 749 F. Supp. 2d 828, 834 (N.D. Ill. Nov. 4, 2010) (holding that statements on company websites are actionable); *see also Muzinich & Co. v. Raytheon*, 2002 U.S. Dist. LEXIS 26962, *11 (D. Idaho Apr. 30, 2002) (broadly interpreting the "in connection with" requirement). Indeed, if any corrective information had been posted on Yahoo's website, Defendants surely would have asserted a truth-on-the-market defense.

The case that Defendants cite involved very different types of communications. *See In re LifeLock Sec. Litig.*, 2017 U.S. App. LEXIS 8386, at *12-13 (9th Cir. May 11, 2017) (holding that print advertisements were inactionable); *compare Carter-Wallace*, 150 F.3d at 156 (holding that detailed "advertisements in sophisticated" journals were actionable). Yahoo's privacy and vulnerability disclosure policies, for example, are not analogous to claims made in print advertisements. These policies were particularly important to investors because Defendants told investors in every periodic filing during the Class Period that data breaches were one of the most significant financial risks that Yahoo faced.[7] Defendants also regularly touted Yahoo's supposedly

[7] *See* ¶¶268-69, 281-82, 294-93, 308-09, 313-14, 326-27, 331-32, 342-43, 349-50, 356-57, 361-62.

high level of security on earnings calls, in press releases, and at prominent conferences.[8] Moreover, the SEC and U.S. Senators recognize the importance of data breaches to investors. ¶¶40, 135. This recognition of cybersecurity's importance to investors belies the notion that investors would not review or care about Yahoo's statements on its website concerning its cybersecurity efforts.

2. The securities fraud claims in the SAC are based on misrepresentations and omissions, not mere mismanagement.

Defendants erroneously argue that the allegations of the SAC constitute claims of only corporate mismanagement. Mot. at 9-10. Defendants committed securities fraud by continually representing that Yahoo disclosed or would disclose significant cybersecurity incidents and that it employed best practices for ensuring the protection of user data while knowingly withholding information about the two largest data breaches in history and the true state of Yahoo's inadequate information security practices. These false and misleading statements related to the core of Yahoo's business constitute more than just mismanagement. *In re Wells Fargo Sec. Litig.*, 12 F.3d 922, 927 (9th Cir. 1993) (corporate management exclusion from § 10(b) is not implicated when plaintiffs allege specific misrepresentations or material nondisclosures in violation of the federal securities laws); *see also Suez Equity Inv'rs, L.P. v. Toronto-Dominion Bank*, 250 F.3d 87, 99 (2d Cir. 2001) (rejecting mismanagement defense where defendants misrepresented "the quality of the proffered securities").

II. The SAC alleges a strong inference that Defendants acted with scienter.

To survive a motion to dismiss, a complaint must allege a "strong inference of scienter." The inference need "not be irrefutable" and plaintiffs may rely upon circumstantial evidence. *In re LDK Solar Sec. Litig.*, 584 F. Supp. 2d 1230, 1241 (N.D. Cal. 2008) (citing *Tellabs*, 551 U.S. 308 (2007)). "Recklessly turning a 'blind eye' to impropriety is equally culpable" to actual knowledge. *In re VeriFone Holdings, Inc. Sec. Litig.*, 704 F.3d 694, 708 (9th Cir. 2012). The relevant inquiry is whether all of the facts alleged, viewed holistically, give rise to a strong inference of scienter. *Tellabs*, 551 U.S. at 326. This inference need only be as compelling as any opposing inference, and "need not be irrefutable, *i.e.*, of the 'smoking-gun' genre." *Id.* at 314, 324. A tie, in which an inference of scienter is

[8] *See* ¶¶244, 252, 254-55, 260, 264, 266, 271-72, 274-75, 277, 279, 284-88, 290, 292, 297-98, 300, 302-04, 306, 311, 316, 318, 320, 322, 324, 329, 334, 336, 338-40, 345-47, 352, 354, 364-67.

equally plausible as competing inferences, therefore goes to the plaintiffs. *Id.* at 324, 328.

In the *Yahoo Customer Data* case, the Court has already credited allegations that Yahoo was "aware of the 2014 Breach as it was occurring in 2014," but acted in bad faith by delaying notifying users for years, leaving them "exposed while [Yahoo] concealed [its] cybersecurity failures until compelled to do so," and by "failing to employ minimal reasonable safeguards." *See* 2017 WL 3727318, at *41, *49. These deliberate actions were particularly indefensible because Yahoo did not provide users the chance to protect themselves by changing their passwords or cancelling their Yahoo accounts. *Id.* The following allegations further support a strong inference of Defendants' scienter.

A. The SAC alleges particularized facts establishing Defendants' knowledge or deliberate recklessness.

Defendants focus their discussion of scienter on when they knew about the Data Breaches. Mot. at 21-30. But Defendants ignore that they had knowledge – from even before the Class Period – of Yahoo's deficient and substandard information security practices that led to the Data Breaches.

1. Defendants were fully aware of Yahoo's deficient information security.

Yahoo's security issues were well known and ignored when Mayer took over as CEO in 2012. ¶90. The Company's long history of breaches put Defendants on clear notice of its vulnerability to hackers and the need to enhance its data security. As one example, in 2010 Google informed Yahoo that its systems were being used to attack Google. ¶63. Following an investigation, Yahoo uncovered that Chinese hackers had penetrated Yahoo's systems prior to 2008. *Id.* Yahoo's inaction resulted in law enforcement authorities notifying Yahoo of a potential breach in 2011, which, tellingly, Yahoo did not address until about January 2012 when it retained an outside security firm to investigate the breach. ¶64. The security firm made "damning" findings and uncovered that two different groups attacked Yahoo's systems starting as early as March 22, 2010. ¶65. In 2012, Yahoo experienced at least two significant security incidents. First, during the release of a plug-in in May 2012, Yahoo inadvertently leaked the private security key that anyone could use to create malicious plug-ins. ¶66. Second, in July 2012, hackers stole over 450,000 unencrypted Yahoo usernames and passwords and posted this data on a public website. ¶67. The hackers that stole this unencrypted user data warned that the breach was a "wake up call" for Yahoo to the "many security holes" in its network. ¶¶67-73.

Security experts expressed concerns about Yahoo's security standards, which further demonstrates Defendants' knowledge of the Company's vulnerabilities. As one example, following the 2012 breach, security experts publicly expressed their shock over Yahoo's inadequate and poor security. More specifically, the hackers used a technique known as SQL injection attack, which as far back as 2003, the Federal Trade Commission considered to be a well-known and foreseeable hacking method and advised companies to take such attacks into account through routine security measures. ¶¶69-72. Also, the stolen user passwords were not encrypted and merely saved in plain text, which security experts were befuddled to learn. ¶72. As another example, cybersecurity firms repeatedly found that Yahoo's security was poor. Between 2013 and 2016, Yahoo retained cybersecurity firms to investigate the Company's issues and vulnerabilities. ¶¶78-82. Each investigation identified numerous vulnerabilities, and each time Yahoo failed to take actions to fix the problems. *Id.*

Criticism about Yahoo's vulnerabilities further shows Defendants were aware of Yahoo's substandard security. In a November 13, 2012 letter to Mayer, industry leaders urged Yahoo to take "the long overdue step of" implementing encryption. ¶74. Some even indicated that they advised their users to avoid Yahoo's mail services "because of its continued lack of essential security protections." ¶74. Moreover, in 2013, Snowden revealed that Yahoo was a frequent target of nation-state spies. ¶91. Likewise, after Yahoo disclosed the 2013 Data Breach in December 2016, news articles strongly criticized Yahoo's lax security measures stating that "[s]ecurity has taken a back seat at Yahoo . . . compared to . . . [its] competitors." ¶104.

The SAC presents substantial evidence that the Individual Defendants were aware of the specific vulnerabilities that allowed the Data Breaches to occur. For example, as stated above, Yahoo failed to protect itself from SQL injection attacks even though such attacks were commonly known as early as 2003. ¶¶69-71. Likewise, as late as the summer of 2013, Yahoo used the MD5 encryption method, even though security experts warned since 2008 that MD5 was cryptographically broken and unsuitable for further use. ¶¶86, 89, 97, 108, 410. Stamos and his information security team repeatedly brought Yahoo's security problems to Mayer's attention. ¶¶89-91, 104. She rejected their proposed improvements because she feared these steps would alienate Yahoo's already tenuous user base. *Id.* This evidence easily raises a strong inference that the Individual Defendants knew of, or were at the

very least deliberately reckless as to, Yahoo's severely inadequate data security practices when Defendants falsely described those measures in glowing terms throughout the Class Period.

This evidence also supports a strong inference that Defendants were deliberately reckless as to the Data Breaches themselves because Defendants failed to take even "the most basic" steps that could have prevented the breaches while knowing that Yahoo was particularly susceptible to attacks by foreign state actors. ¶¶71-73, 83-87, 89-94, 104. Defendants' deliberate disregard of security deficiencies when the risk they posed was well known is a paradigmatic example of the type of deliberate recklessness that supports scienter. *See Howard v. Everex Sys.*, 228 F.3d 1057, 1064 (9th Cir. 2000) ("potential alarm signals in the face of Everex's possible financial crisis" supported scienter); *Kiernan v. Homeland, Inc.*, 611 F.2d 785, 788 (9th Cir. 1980) (failure to investigate supported scienter); *In re BP Prudhoe Bay Royalty Tr. Sec. Litig.*, 2007 U.S. Dist. LEXIS 83007, at *12 (W.D. Wash. Oct. 26, 2007) (finding scienter based on red flags concerning poor quality of pipelines). Once the Data Breaches occurred, the Company's conduct was particularly galling. Instead of requiring users to simply change their usernames and passwords, Yahoo opted to leave 3 billion of its customers exposed to hackers' data theft.

2. The SAC alleges that Defendants knew about or recklessly ignored the 2013 Data Breach.

Defendants contest scienter as to the 2013 Data Breach by asserting that Defendants did not have knowledge of the 2013 Data Breach prior to 2016 and therefore could not have acted with scienter. Mot. at 22-23. However, the SAC presents a slew of evidence raising strong inference that Defendants were aware of, or deliberately reckless in not knowing of, the 2013 Data Breach.

The 2013 Data Breach occurred in August 2013. ¶97. Hackers breached Yahoo's email system, stealing the records of billions of users, including names, birth dates, phone numbers, passwords, and even the security questions and backup email addresses used to reset lost passwords. *Id.* The hackers forged the cookies that Yahoo placed on user computers, including authentication cookies, which allowed them to gain access to email accounts without ever having users' passwords and to remain logged in to users' accounts indefinitely. *Id.* The 2013 Data Breach was a result of Yahoo's failure to timely move away from the outdated MD5 encryption technology, which long

before had been widely recognized in the data security industry as "cryptographically broken and unsuitable for further use." ¶¶86, 89, 97, 108, 410.

The resulting 2013 Data Breach was catastrophic: It remains the largest data breach from a single site in history, dubbed "the Exxon Valdez of security breaches." ¶¶107, 236. Illustrating its magnitude, one analyst said that "1 billion accounts [were] compromised, when there [were] only 3 billion people with Internet access in the world." ¶107. Yet Defendants failed to disclose the breach until more than three years later, on December 14, 2016, and only after federal authorities confronted the Company about it. ¶102. It was later disclosed that all 3 billion accounts were compromised. ¶2.

Either Defendants knew about the 2013 Data Breach or they recklessly failed to timely identify and publicly disclose its existence. As alleged in the SAC, a confidential witness ("CW1"), who was part of Yahoo's security team between 2010 and 2014, stated that the Company knew about the 2013 Data Breach as it occurred. ¶¶210-12. Specifically, Yahoo suffered two significant Data Breaches during CW1's time at Yahoo. ¶211. In response to those breaches, the security team went "into damage control and pull[ed] a lot of resources" to take care of the breaches. *Id.* Mayer was aware of the breaches and "wanted to stay in the loop on the team's progress" in addition to the daily meetings and updates. *Id.* However, Mayer "definitely didn't want to publicize [the breaches]." ¶212.

Yahoo discontinued the use of the antiquated MD5 encryption protocol in the summer of 2013. ¶410. This is precisely the time that the 2013 Data Breach occurred. *Id*. It strains credulity to suggest that this remedial measure was not taken in response to the breach. Indeed, Yahoo's MD5 sub-standard encryption was said to have contributed to the 2013 Data Breach. ¶¶96-97.

The SAC alleges that even if Defendants did not have contemporaneous *actual* knowledge of the 2013 Data Breach, they recklessly failed to timely identify the attack. As discussed above, at the time of the 2013 Data Breach, Defendants knew that MD5 was outdated encryption and unsuitable for further use, and yet the user data stolen in the 2013 Data Breach was encrypted with the easily broken MD5 security. ¶¶86, 97. As such, Defendants knew of the vulnerability. Further, according to multiple data security experts, it takes an average of 191 to 201 days to detect a data breach, and this period is usually shorter for technology-focused companies such as Yahoo. ¶¶219-20. As evidence of Defendants' reckless disregard of the 2013 Data Breach, InfoArmor, a cybersecurity firm totally

separate from Yahoo, independently identified the breach. ¶¶98-99. When InfoArmor approached Yahoo about the breach months before it was disclosed to the public, the Company was dismissive. ¶101. After being rebuffed by Yahoo, InfoArmor notified military and law enforcement authorities in the United States and several other countries about the breach, some of which confronted Yahoo with their concerns. *Id.* After the breach was disclosed, the chief executive of a security company told the press that "[w]hat's most troubling is that this occurred so long ago, in August 2013, and no one [supposedly] saw any indication of a breach occurring until law enforcement came forward." ¶104.

This evidence raises a strong inference that Defendants knew of the 2013 Data Breach, or were at the very least deliberately reckless in failing to discover the 2013 Data Breach, as Defendants falsely described Yahoo's measures for ensuring users' privacy and security in glowing terms throughout the Class Period.

3. Defendants acknowledge that senior Yahoo executives had contemporaneous knowledge of the 2014 Data Breach.

The SAC presents overwhelming evidence demonstrating that Defendants had contemporaneous knowledge of the 2014 Data Breach. Because Defendants cannot seriously contest that they had knowledge of Yahoo's substandard security practices and the Data Breach, they resort to rehashing their futile arguments already addressed above as to falsity and materiality. Mot. at 23-29.

In the 2014 Data Breach, Russian state-sponsored hackers stole the account information of 500 million Yahoo users, including names, e-mail addresses, telephone numbers, dates of birth, passwords (created with MD5 algorithms), and security questions and answers. ¶108. The hackers laid the groundwork for this data breach in early 2014, when they gained unauthorized access to Yahoo's network and stole its user database and account management tools. ¶111.

Defendants knew about the 2014 Data Breach while it was occurring and yet, shockingly, Yahoo concealed this information from its customers and investors for approximately two years, finally disclosing the breach on September 22, 2016. ¶185. Critically, Defendants' own disclosures acknowledge that Yahoo had "identified [the 2014 Data Breach] in late 2014." ¶¶195, 203. The Independent Committee's investigation revealed that Defendants had contemporaneous knowledge of the 2014 Data Breach. ¶204. The Committee found that Yahoo's information security team, which

was led by Stamos at the time, had "contemporaneous knowledge" of the 2014 Data Breach." ¶204. Specifically, by "late 2014, senior executives and relevant legal staff [*i.e.*, Bell's team] were aware that a state-sponsored actor had accessed certain user accounts by exploiting the Company's account management tool." *Id.* Despite this contemporaneous knowledge, "certain senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon, the full extent of knowledge known internally by the Company's information security team." *Id.* Even if this self-serving finding were accepted as true, it is a textbook example of recklessness, especially given Yahoo's history of breaches.

The findings of the Independent Committee actually *understate* Defendants' contemporaneous knowledge of the 2014 Data Breach. As early as October 9, 2014, Yahoo's information security team, led by Stamos, detected the presence of Russian hackers in the Company's systems. ¶131. Stamos and his team investigated the breach, which it named "Siberian Intrusion," and tracked the hackers' movement until at least February 2015. ¶¶130-31. Realizing the severity of the Siberian Intrusion, on November 14, 2014, Yahoo engaged a third-party forensic expert to aid with the investigation. ¶139. Around December 2014, the information security team found, and the third-party forensic expert confirmed, that Russian hackers had in fact exfiltrated Yahoo user data. ¶¶142-43. Defendants knew soon after the breach that with respect to the data compromised, "[*b*]*est case scenario" was that "108M [million] credentials in UDB" were "compromised." The "[w]orst case scenario" was that "[a]ll credentials in UDB" were "compromised*." ¶145.

The information security team routinely updated Yahoo's management and the Board about the Siberian Intrusion. *See, e.g.*, ¶¶123-63. As standard procedure, Yahoo's Board, which included Mayer, and the Audit and Finance Committee of the Board ("AFC"), received regular security updates from Stamos' data security team. ¶¶123-25. During the Class Period, the Board or the AFC received data security updates during at least fourteen separate meetings between April 2014 through April 2016. ¶¶125, 127. Thus, the Board and the AFC learned about the 2014 Data Breach during these meetings. More tellingly, the information security team held daily meetings for months to discuss and analyze the Siberia Intrusion. ¶134. According to Stamos and Ramses Martinez ("Martinez"), a senior member of the information security team, the information security team routinely updated Yahoo's

management, the Board, and the AFC about its findings and conclusions regarding the Siberian Intrusion. ¶135-36. Specifically, during some of these meetings, Stamos provided extensive reporting to Bell and Mayer, among other members of Yahoo's management. ¶¶134, 149-50. According to Stamos, all material facts were reported and there was ample knowledge within Yahoo regarding the 2014 Data Breach. ¶148. Indeed, Board materials from October 15, 2014, April 15, 2015, and June 23, 2015, show that detailed information about the Siberia Intrusion was provided to the AFC. ¶152.

Stamos testified that Bell and Mayer had contemporaneous knowledge of the Siberia Intrusion, including the fact that a massive number of Yahoo accounts had been compromised. ¶151. Others with firsthand knowledge have explained that Mayer was personally involved in efforts to resolve the Data Breaches and knew of their severity when they occurred. CW1 stated that Mayer was updated on the two data breaches on a daily basis. ¶211. The FBI agent in charge of investigating the 2014 Data Breach stated at a March 15, 2017 press conference that Mayer "and her team at Yahoo" were "great partners" during their *two-year investigation*. ¶205.

4. Defendants acknowledge that senior Yahoo executives had contemporaneous knowledge of the Forged Cookie Breach.

The SAC presents ample evidence demonstrating that Defendants had contemporaneous knowledge of the Forged Cookie Breach. The Forged Cookie Breach occurred in 2015 and 2016, was related to the 2014 Data Brach, and facilitated by the data stolen in the 2014 Data Breach. ¶¶197, 99. Approximately 32 million Yahoo users appear to have been affected. *Id.* The Independent Committee's investigation found that the Company "had contemporaneous knowledge of the . . . cookie forging in 2015 and 2016." ¶204. However, the Forged Cookie Breach was not disclosed until March 1, 2017, when Yahoo informed the affected users that "[w]e believe an unauthorised third party accessed the company's proprietary code to learn how to forge certain cookies." ¶197. As Yahoo explained, "[f]orged cookies could allow an intruder to access users' accounts without a password." *Id.* The Company has connected the Forged Cookie Breach to the same Russian state-sponsored hackers responsible for the 2014 Data Breach. *Id.*

B. Additional allegations in the SAC bolster a strong inference of scienter.

Additional evidence highlighting the suspicious nature of the Individual Defendants' actions

bolsters the strong inference of scienter as to their concealment of Yahoo's deficient and substandard information security and the occurrence of the Data Breaches. Martinez testified that the legal department ordered him to keep details of his presentations to the Board about the 2014 Data Breach out of any written materials presented to the Board to avoid creating a paper trail. ¶¶153-57. Congress, law enforcement agencies, and industry experts found it "strange" and "deeply troubling" that it took Defendants so long to disclose the breaches when these types of incidents are usually discovered much sooner. ¶¶194-95, 219-29, 394, 398. They did not believe that Yahoo's top executives did not know about the breaches when they occurred. *Id.* Senator Mark Warner even told the SEC that Yahoo's "assert[ed] lack of knowledge . . . creates serious concerns about truthfulness in representations to the public." ¶223. Multiple government agencies have opened investigations into what Yahoo executives knew and when, including the unprecedented step of a criminal investigation related to cybersecurity disclosures. ¶¶225-27. *See In re Gentiva Sec. Litig.*, 932 F. Supp. 2d 352, 380 (E.D.N.Y. 2013) (government investigations add to inference of scienter).

Defendants' continued deceit as the Class Period wore on further supports a strong inference of scienter. *Reese v. Malone*, 747 F.3d 557, 572 (9th Cir. 2014) (scienter is supported where defendants make "detailed factual statement[s], contradicting important data to which [they] had access"). Mayer and Yahoo blatantly misrepresented in SEC filings as late as September 2016 – after Mayer was already working with the FBI and knew that third parties had approached the Company with information concerning the Data Breaches (¶¶98-101, 171-73, 205-07) – that Yahoo had not suffered any material data breaches and was not subject to any related government investigations. ¶¶223, 368. And in May 2015, Mayer was asked about how Yahoo responded to Snowden's revelation that Yahoo had been subject to hacks by foreign state actors. ¶¶91, 316. Rather than answering truthfully that, at that very moment, Yahoo user information was being accessed by Russian state hackers, Mayer falsely reassured the public that users could trust in Yahoo's encryption methods. ¶316. Similarly, the Court has credited allegations that Yahoo has "not only failed to take any actions with regard to [user] information being [sold] on the dark web, but [has] continued to dispute the scope of [its] responsibility." *Yahoo Customer Data*, 2017 WL 3727318, at *31. Stamos and Bell also repeatedly vouched for the safety of users' data, with Stamos testifying before Congress about

Yahoo's industry-leading efforts, and Bell describing "the security of [Yahoo] users' information [as being] of paramount importance." ¶¶284-88, 352. Defendants' repeated false praise of Yahoo's security efforts while knowing those efforts were severely deficient and resulted in the Data Breaches, supports a strong inference that they acted with culpable, rather than innocent, intent. *Reese*, 747 F.3d at 572; *Roberti v. OSI Sys., Inc.*, 2015 U.S. Dist. LEXIS 24761, at *30 (C.D. Cal. Feb. 27, 2015) (scienter was supported "by the fact that the Defendants touched on the" issue in public statements).

The fact that Mayer and her team reported the 2014 Data Breach to the FBI also shows that they understood its importance. In fact, Alexsey Belan, one of the hackers that perpetrated the attack, was on the FBI's list of Cyber Most Wanted criminals since 2012 because of his prior hacks of millions of accounts at major e-commerce companies. ¶113. Defendants cannot plead ignorance of the severity of the Data Breaches when they were aware of Yahoo's history of breaches by foreign state actors and reported the 2014 Data Breach to the FBI.

Defendants cite the Independent Committee's attribution of Yahoo's mishandling of the 2014 Data Breach to "failures in communication, management, inquiry and internal reporting" rather than intentional misconduct. Mot. at 25. But this vague, self-serving assertion raises more questions than answers and fails to account for the additional evidence described herein that the Committee has not been able to explain. Moreover, such abjectly poor internal controls would be yet another red flag that supports scienter. *Everex Sys.*, 228 F.3d at 1064.

The Individual Defendants have all been penalized or left the Company as a result of the Data Breaches and Yahoo's security deficiencies. Based on the Independent Committee's investigation, Bell was forced to resign without pay and Mayer lost her cash bonus for 2016 and her annual equity award for 2017. ¶¶204. Stamos quit because he "repeatedly clashed" with Mayer over her refusal to take measures to improve cybersecurity. ¶93. Executive resignations under suspicious circumstances are evidence of scienter. *In re Volkswagen*, 2017 U.S. Dist. LEXIS 1109, at *840-41 (N.D. Cal. Jan. 4, 2017); *In re Adaptive Broadband Sec. Litig.*, 2002 U.S. Dist. LEXIS 5887, at *43 (N.D. Cal. 2002).

Defendants' claim that Mayer's and Bell's penalties were not a result of culpable involvement in Yahoo's failure to address the 2014 Data Breach (Mot. at 25, 27) strains credulity. Yahoo itself described these penalties as being in direct response to the Independent Committee's findings related

to the 2014 Data Breach. ¶204. The inference that Mayer and Bell were penalized because they were aware of the breach but failed to respond appropriately is at least as compelling as any alternative inference. Indeed, it's the only plausible inference.

As supposedly exculpatory evidence, Defendants point to the risk warning in Yahoo's SEC filings that "[s]ecurity breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure." Mot. at 24. Defendants argue that this disclosure is "inconsistent with a strong inference that Ms. Mayer sought to deceive investors." *Id.* But this boilerplate statement of risk failed to enlighten investors in any meaningful way, as it was vague and obvious, especially to anyone aware of Yahoo's long history of breaches before the Class Period. Moreover, the disclosure was itself materially misleading because it failed to warn that Yahoo's information security was substandard and that the risk had already materialized in the form of two of the largest breaches in history. Thus, this statement was entirely consistent with deceptive intent.

C. The core operations doctrine further supports scienter.

Scienter may be imputed to Defendants under the "core operations" doctrine based on "allegations regarding management's role in [the] company." *S. Ferry LP, No. 2 v. Killinger*, 542 F.3d 776, 785-86 (9th Cir. 2008). Such allegations may support scienter in any one of three ways: (i) generalized allegations may be combined with other evidence to raise a strong inference of scienter; (ii) particularized allegations may independently raise a strong inference of scienter when they "suggest that defendants had actual access to the disputed information"; and (iii) allegations even "in a more bare form" may raise a strong inference of scienter where "it would be 'absurd' to suggest that management was without knowledge." *Id.* All three ways apply here.

As CEO, Mayer was responsible for Yahoo's most important operations. She told investors in every periodic filing during the Class Period that data breaches were one of the most significant risks that Yahoo faced; Yahoo's history of breaches was one of the main problems she confronted; and she often discussed Yahoo's cybersecurity practices. *See supra* at 11, 13. As Yahoo's CISO, Stamos reported directly to Mayer, his sole function was to oversee cybersecurity, and he was the public face of these efforts. ¶¶17, 284-88, 297-98. Bell, as GC, described the Legal Department's "main job" as protecting the security of Yahoo's users. ¶¶271, 352. These allegations, in combination with all of the

others described above, support a strong inference that the Individual Defendants knew the details of Yahoo's cybersecurity efforts. *Reese*, 747 F.3d at 575-77 (scienter sufficiently alleged as to officer who oversaw company's operations at issue).

The SAC pleads particularized allegations showing that each of the Individual Defendants had access to information relating to the Data Breaches and to Yahoo's deficient cybersecurity practices. The Independent Committee found that Yahoo's information security team had full knowledge of the 2014 Data Breach in late 2014, and that the legal team also mishandled the breach. ¶¶204, 213. Stamos and Bell, who were in charge of these departments, thus had access to this information. The Committee also determined that Mayer had knowledge of at least some aspects of the 2014 Data Breach in late 2014. ¶204. She also had ready access to the information held by the security and legal teams. Stamos and his team gave regular updates to the Board following the breaches, and Company policy required weekly updates to Mayer on security bugs. ¶¶123-25, 294-95. Stamos and Mayer "repeatedly clashed" over Yahoo's failure to cure its information security deficiencies. ¶92. These allegations independently support a strong inference of scienter. *South Ferry*, 542 F.3d at 786; *Malone*, 747 F.3d at 576. CW1's observation of Mayer's detail-oriented management style further supports scienter. ¶¶210-11; *Oracle Corp.*, 380 F.3d at 1234.

Lastly, given Yahoo's glaring information security deficiencies, the ready availability of information about the Data Breaches from Yahoo's information security team and third parties scouring the internet, and the clear notice Defendants had received that Yahoo was regularly susceptible to being hacked by foreign state actors, it is "absurd" to suggest that the Individual Defendants did not know about these matters or discuss them with employees who did. *See No. 84 Employer-Teamster Joint Council Pension Tr. Fund v. America W.*, 320 F.3d 920, 943 n.21 (9th Cir. 2003) (holding it was "absurd" to suggest that the Board did not discuss safety problems and government investigation that were very important to the airline); *Mulligan*, 36 F. Supp. 3d at 969-70.

D. Defendants had a concrete financial motive to mislead investors.

Although "motive is not required to adequately plead scienter," it supports a strong inference of culpability. *Gammel v. Hewlett-Packard Co.*, 2013 U.S. Dist. LEXIS 68026, *59 (C.D. Cal. May 8, 2013); *Everex Sys.*, 228 F.3d at 1064-1065. Mayer deliberately chose to focus on other priorities that

conflicted with improving Yahoo's cybersecurity efforts. For her, "defending against hackers took a back seat at Yahoo" because she did not want to alienate Yahoo's users by slowing down its services or by instructing users to change their passwords. ¶¶91-93. As CW1 explained, Mayer "definitely didn't want to publicize" the Data Breaches. ¶212. After all, "data controllers have little incentive to disclose breaches voluntarily, given the possible harm this can cause to their reputation." ¶38. By hiding the massive Data Breaches and refusing to improve its security measures, Yahoo was able to retain users who were duped into believing that its services were secure. ¶62. This was particularly important to Mayer because one of Yahoo's largest shareholders was pressuring Yahoo to sell its operating business or replace the Board (including Mayer) with new Directors. ¶¶50-52, 382.

Defendants concealed the Data Breaches in part to facilitate the sale of Yahoo's operating business. ¶¶417, 194. *See Yahoo Customer Data*, 2017 WL 3727318, at *3 ("Plaintiffs allege that Yahoo delayed notifying users or the public about the 2014 Breach while 'Yahoo solicited offers to buy the company. Reportedly, Yahoo wanted the offers in by April 19, 2016,' and thus waited to disclose the breach until September 2016."). Defendants' actions, taken at the direct expense of users to bolster Yahoo's appeal to Verizon and insulate Mayer's job from dissident investors, go far beyond an ordinary desire for the company to do well. *See Nguyen v. Radient Pharm.*, 2011 U.S. Dist. LEXIS 122533, at *24-26 (C.D. Cal. Oct. 20, 2011) (motive alleged where "ability to continue operating was dependent upon raising additional capital"); *LDK Solar*, 584 F. Supp. 2d at 1247 (motive to misstate financials to attract investors in highly competitive market).

Mayer was also financially motivated to misrepresent Yahoo's security infirmities and conceal the Data Breaches. She was paid $186 million during the Class Period, including $51 million from the sale of Yahoo stock at prices that she knew did not reflect the Company's true value. She also stood to receive a $23 million golden parachute from the Verizon deal. ¶215. These concrete financial benefits show Mayer's financial motive to conceal the Data Breaches. *Nursing Home Pen. Fund, Local 144 v. Oracle Corp.*, 380 F.3d 1226, 1232 (9th Cir. 2004).

E. The SAC alleges Yahoo's corporate scienter.

Because the SAC adequately pleads scienter as to each of the Individual Defendants, scienter is imputed to Yahoo. *Robb v. Fitbit*, 2017 U.S. Dist. LEXIS 7722, at *20 (N.D. Cal. Jan. 19, 2017). In

the Ninth Circuit, scienter may also be imputed to a company, even if it is not sufficiently alleged as to any individual, where the "company's public statements were so important and so dramatically false that they would create a strong inference that at least *some* corporate officials knew of the falsity upon publication." *In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1063 (9th Cir. 2014); *Volkswagen*, 2017 U.S. Dist. LEXIS 1109, at *838-41; *Fitbit*, 2017 U.S. Dist. LEXIS 7722, at *17-20.

The falsity of Defendants' positive descriptions of Yahoo's information security practices and the misleading nature of their failure to disclose the Data Breaches while touting compliance with state and federal legal obligations to do so, was obvious, and these issues were of vital importance to Yahoo's business. Moreover, the Independent Committee found that several individuals and groups within the Company knew about and mishandled the 2014 Data Breach. ¶¶204, 213. Thus, "at least *some* corporate officials knew" these statements were false and misleading when they were made.

Most of the cases cited by Defendants (Mot. at 29-30) predate the Ninth Circuit's decision in *Glazer* that allowed for collective scienter. 549 F.3d at 743.[9] The only cited post-*Glazer* cases within the Ninth Circuit either do not address collective scienter or acknowledge that collective scienter might be valid but dealt with alleged fraud that was far less significant to the company's business than the Data Breaches here. *See In re ChinaCast Educ. Corp. Sec. Litig.*, 809 F.3d 471, 476 (9th Cir. 2015); *Okla. Firefighters Pension & Ret. Sys. v. IXIA*, 50 F. Supp. 3d 1328, 1354 (C.D. Cal. 2014).

III. The SAC adequately alleges loss causation and damages.

Loss causation is properly pleaded with a showing "that the revelation of [the defendant's] misrepresentation or omission was a substantial factor in causing a decline in the security's price." *Nuveen Mun. High Inc. Opp. Fund v. City of Alameda*, 730 F.3d 1111, 1119 (9th Cir. 2013). There is no single method by which loss causation must be alleged because all that is required is "that the defendants' misrepresentation (or other fraudulent conduct) proximately caused the plaintiff's economic loss." *Dura Pharms., Inc. v. Broudo*, 544 U.S. 336, 346 (2005). Loss causation is therefore generally "a matter of proof at trial and not to be decided on a Rule 12(b)(6) motion to dismiss." *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1057 (9th Cir. 2008). The Ninth Circuit recently clarified that

[9] Defendants cite *Weiss v. Amkor Tech., Inc.*, 527 F. Supp. 2d 938 (D. Ariz. 2007), but they mistakenly date the decision from 2017.

loss causation can be shown through a series of partial corrective disclosures that together show that when the truth "began to leak out, it caused the price of stock to depreciate." *Lloyd v. CVB Fin. Corp.*, 811 F.3d 1200, 1210 (9th Cir. 2016). A corrective disclosure "need not precisely mirror the earlier misrepresentation." *Id.* Loss causation may also be pled under the "materialization of the concealed risk" approach, whereby the misstatements and omissions at issue concealed a risk that ended up materializing and "played some part in diminishing the market value of a security." *Nuveen*, 730 F.3d at 1120; *In re Charles Schwab Corp. Sec. Litig.*, 257 F.R.D. 534, 542, 547 (N.D. Cal. Feb. 4, 2009).

There is a market damage amount of $350 million, constituting the price reduction given to Verizon upon learning of the breach. Yahoo's investors suffered significant damages in 2015 and 2016 through a series of related disclosures, including Defendant Stamos' departure, followed by the $4.46 billion write-down. Moreover, history has a tendency to repeat itself and we have seen this in another Alex Stamos departure, this time with Facebook. Approximately $60-80 billion in market capitalization evaporated at Facebook (where the accounts of 50 million users were breached – 1/20 the size of Yahoo's).

A. The SAC alleges loss causation as to Maher.

The SAC alleges multiple corrective disclosures that took place before Maher's positions in Yahoo securities expired on February 19, 2016. For example, on May 18, 2015, it was reported that Yahoo's Chief Information Officer, Mike Kail, left the Company after less than one year. ¶373. This surprising news led to Yahoo's stock price dropping $3.38, or 7.6%, the following day. ¶374. Then, on Friday, September 11, 2015, TechCrunch reported that Yahoo's interim CISO left the Company after serving in that role for only two months, having been appointed to that role in July, when Stamos resigned as CISO. ¶377. The resignation of an employee responsible for the subject matter of defendants' misrepresentation suffices to show loss causation at the pleading stage. *Cement & Concrete Workers Dist. Council Pension Fund v. Hewlett Packard*, 964 F. Supp. 2d 1128, 1145-46 (N.D. Cal. 2013) (CEO's resignation "was a materialization of the previously undisclosed risks").[10]

Other disclosures revealed the negative consequences of Yahoo's information security

[10] In addition, on September 14, 2015, it was reported that Yahoo Messenger suffered from a serious security bug susceptible to hackers. ¶378. That day, Yahoo's share price fell $1.11, or 3.53%. ¶379.

deficiencies and the Data Breaches. On February 2, 2016, Yahoo disclosed a $4.46 billion goodwill impairment due to a substantial decrease in the value of Yahoo's operating business severely harmed by the Data Breaches, resulting in a $1.38, or 4.75%, stock drop the following day. ¶¶388-89. This and other disclosures alleged in the SAC support loss causation because they revealed the foreseeable negative consequences of Defendants' false and misleading statements. *Lloyd*, 811 F.3d at 1210; *In re Daou Sys.*, 411 F.3d 1006, 1026 (9th Cir. 2005); *Charles Schwab*, 257 F.R.D. at 542, 547.

B. The SAC alleges damages as to Sutton View and Talukder

Sutton View, like Maher, suffered losses when disclosures partially revealed Defendants' fraud, and Defendants do not dispute that Sutton View held Yahoo shares through the end of the Class Period. Defendants' only argument is that these shares were purchased below the PSLRA's 90-day lookback threshold. Mot. at 32-33. This argument fails because application of the 90-day lookback involves complex damages issues that cannot be considered on a motion to dismiss. *Mausner v. Marketbyte LLC*, 2013 U.S. Dist. LEXIS 199521, *34 (S.D. Cal. Jan. 4, 2013) (holding the 90-day lookback "only relates to the maximum amount of damages"); *In re Terayon Communs. Sys.*, 2003 U.S. Dist. LEXIS 2852, *8 (N.D. Cal. Feb. 24, 2003) (same at class certification). None of the cases that Defendants cite are relevant because they were all decided after the pleading stage.

As for Talukder, Defendants acknowledge that he made several purchases of hundreds of shares at prices above the 90-day lookback threshold that he held through the end of the Class Period. Mot. at 33. Defendants claim that these purchases, which were made by November 6, 2014, came before the 2014 Data Breach. But the hackers attacked Yahoo's AMT in October 2014, expanded their attack to Yahoo's UDB in November 2014, and began their reconnaissance even earlier in 2014. ¶¶114. 130-32. Talukder thus purchased shares after Defendants are alleged to have known about the 2014 Data Breach. Moreover, Defendants knew of Yahoo's inadequate information security from the start of the Class Period and had contemporaneous knowledge of the 2013 Data Breach, supporting additional misstatements and omissions that took place before Talukder's purchases.

C. The SAC has alleged loss causation as to the misrepresentations and omissions in the Stock Purchase Agreement.

Defendants argue that Plaintiffs cannot bring their claims as to the misstatements in the

Verizon SPA because none of the Plaintiffs purchased shares after the agreement was filed with the SEC. Mot. at 18. But where, as here, a plaintiff "has individual standing as to some claimed injuries of the class," the plaintiff has standing on behalf of the entire class. *In re Connetics Corp. Sec. Litig.*, 542 F. Supp. 2d 996, 1004 (N.D. Cal. 2008); *see also In re Symbol Techs., Inc. Sec. Litig.*, 2013 U.S. Dist. LEXIS 171688 at *52-53 (E.D.N.Y. Dec. 5, 2013) (plaintiff had standing to sue on misrepresentations made before or after its purchases); *In re VeriSign*, 2005 U.S. Dist. LEXIS 10438, at *10-11 (N.D. Cal. Jan. 13, 2005). All of Plaintiffs' claims arise out of the same fraudulent scheme related to the Data Breaches and Yahoo's deficient information security practices, and each of the Plaintiffs has standing with respect to at least some of the claims. Each Plaintiff may therefore bring all of the claims in the SAC on behalf of the class.

IV. The SAC adequately alleges control person liability.

Defendants do not dispute that Plaintiffs have adequately alleged that Mayer is a control person for purposes of Section 20(a). Mot. at 34-35. Defendants are incorrect, however, that the allegations against Bell and Stamos are based solely on their positions. *Id.* Stamos was in charge of Yahoo's information security team (which the Independent Committee found had full knowledge of the 2014 Data Breach), reported directly to Mayer, and was the public face of the Company's security practices before Congress and elsewhere. ¶¶17, 284-88, 297-98. The Committee also found that the legal team, which Bell oversaw, "had sufficient information to warrant substantial further inquiry in 2014," and failed to pursue it. ¶213. Bell lost his job because of his responsibility for this failure. *Id.* He also reassured the public that the Legal Department's "main job" was to protect the data security of Yahoo's users. ¶204, 271. Both Bell and Stamos therefore exercised control over Yahoo's statements related to its cybersecurity practices and the Data Breaches. Under Ninth Circuit law, nothing more is required to plead Section 20(a) liability. *See Everex Sys.*, 228 F.3d at 1065.

CONCLUSION

For all of the foregoing reasons, Defendants' Motion should be denied in its entirety.

DATED: March 30, 2018

GLANCY PRONGAY & MURRAY LLP

By: */s/ Joshua L. Crowell*

Joshua L. Crowell
Vahe Mesropyan
1925 Century Park East, Suite 2100
Los Angeles, California 90067
(310) 201-9150
jcrowell@glancylaw.com
vmesropyan@glancylaw.com

POMERANTZ LLP
Jeremy A. Lieberman
Emma Gilmore
Michael Grunfeld
600 Third Avenue, 20th Floor
New York, New York 10016
(212) 661-1100
jalieberman@pomlaw.com
egilmore@pomlaw.com

Patrick V. Dahlstrom
Ten South La Salle Street, Suite 3505
Chicago, Illinois 60603
(312) 377-1181
pdahlstrom@pomlaw.com

Counsel for Plaintiffs and Lead Counsel for the Class

BRONSTEIN, GEWIRTZ & GROSSMAN, LLC
Peretz Bronstein
60 East 42nd Street, Suite 4600
New York, New York 10165
(212) 697-6484
peretz@bgandg.com

Additional Counsel for Plaintiffs

PROOF OF SERVICE BY ELECTRONIC POSTING

I, the undersigned say:

I am not a party to the above case, and am over eighteen years old. On March 30, 2018, I served true and correct copies of the foregoing document, by posting the document electronically to the ECF website of the United States District Court for the Northern District of California, for receipt electronically by the parties listed on the Court's Service List.

I affirm under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on March 30, 2018, at Los Angeles, California.

s/ Joshua L. Crowell
Joshua L. Crowell

Mailing Information for a Case 5:17-cv-00373-LHK In Re Yahoo! Inc. Securities Litigation

Electronic Mail Notice List

The following are those who are currently on the list to receive e-mail notices for this case.

- **Edward Andrew Bayley**
  ebayley@keker.com,laure-mandin-6675@ecf.pacerpro.com,lmandin@keker.com,efiling@keker.com,ed-bayley-0392@ecf.pacerpro.com
- **Martha A Boersch**
  mboersch@boerschshapiro.com,lkollios@boerschshapiro.com,rvorkoeper@boerschshapiro.com,frizvi@boerschshapiro.
- **Joshua L Crowell**
  jcrowell@glancylaw.com,joshua-crowell-3496@ecf.pacerpro.com,dmanning@glancylaw.com
- **Jordan Eth**
  jeth@mofo.com,jordan-eth-3756@ecf.pacerpro.com,tkhadoo@mofo.com,trina-khadoo-5939@ecf.pacerpro.com
- **Emma Gilmore**
  egilmore@pomlaw.com,egoodman@pomlaw.com
- **Jo W. Golub**
  jgolub@keker.com,sandy-giminez-6735@ecf.pacerpro.com,SHarmison@keker.com,efiling@keker.com,jah@keker.com,jo-golub-8129@ecf.pacerpro.com
- **Michael Grunfeld**
  mgrunfeld@pomlaw.com
- **J Alexander Hood , II**
  ahood@pomlaw.com,abarbosa@pomlaw.com
- **Lara Kollios**
  lkollios@boerschshapiro.com,dshapiro@boerschshapiro.com,rvorkoeper@boerschshapiro.com,mboersch@boerschshap
- **Adam G. Kurtz**
  agkurtz@pomlaw.com
- **Jennifer Michelle Leinbach**
  jleinbach@glancylaw.com
- **Jeremy A Lieberman**
  jalieberman@pomlaw.com,disaacson@pomlaw.com,abarbosa@pomlaw.com,lpvega@pomlaw.com
- **Judson Earle Lobdell**
  jlobdell@mofo.com,magdalena-blackmer-3352@ecf.pacerpro.com,judson-lobdell-6493@ecf.pacerpro.com,mblackmer@mofo.com
- **Jennifer Pafiti**
  jpafiti@pomlaw.com,kmsaletto@pomlaw.com,disaacson@pomlaw.com,abarbosa@pomlaw.com
- **Robert Vincent Prongay**

Manual Notice List

The following is the list of attorneys who are **not** on the list to receive e-mail notices for this case (who therefore require manual noticing). You may wish to use your mouse to select and copy this list into your word processing program in order to create notices or labels for these recipients.

- (No manual recipients)